Ethical Implications of the Snowden Revelations

Draft 12 for IJISPA **(International Journal of Intelligence, Security, and Public Affairs)**

Michael Andregg, University of St. Thomas and University of Minnesota, St. Paul, Minnesota, USA.
mmandregg@stthomas.edu

abstract

This paper addresses a number of ethical dilemmas and practical consequences of the revelations of Edward Snowden about massive electronic surveillance of telephone calls, emails, social media posts and other "Signals Intelligence" (or SIGINT) across the entire world, but especially including domestic American communications formerly thought immune to such surveillance unless authorized by judicial warrant. Practical consequences matter for all "utilitarian" ethical judgments. The author concludes that by far the largest issue is whether US intelligence professionals regard the US Constitution as supreme law in America, or non-disclosure contracts with individual agencies or the US government. Reactions to Snowden follow this pattern, with security cleared insiders generally considering him a traitor, and ordinary people generally considering him a hero for telling the public about illegal activity within the National Security agency directed against fundamental, and constitutionally protected civil liberties like freedom of speech.

Introduction

The most profound ethical question raised by revelations by Edward Snowden of vast increases in National Security Agency (NSA) surveillance, both foreign and domestic, is which is more important: An oath before God to preserve, protect and defend the US Constitution, or contracts with government agencies to guard every secret so classified from disclosure, even if those secrets suggest pervasive violations of the Constitution? This is the fissure that divides many practitioners, who think that Snowden is a traitor to their agencies and perhaps even to the people

at large, and a great many outsiders who think that Snowden is a hero for revealing massive wrongdoing under color of authority, shielded by excessive secrecy. Secondary ethical questions arise from many consequences of the Snowden revelations. Intelligence agents and organizations are generally far more responsive to consequential or utilitarian ethics than to rule based (deontological) systems and probably least to Aristotelian virtue ethics. Therefore this paper will march through eight other practical and ethical questions presented by the Snowden Revelations.

Eight Secondary Practical and Ethical Questions Include:

-- How have Snowden's disclosures affected journalism, and the ability of free people to know what governments are doing?

-- Have they affected 'whistleblowers' in particular, and is that good or bad?

-- How much have those disclosures armed real and potential enemies by warning them about communications intercept and manipulation capabilities, versus how much have they enhanced accountability by warning publics about how far governments can, and do, evade law secretly?

-- Have these capabilities empowered propaganda or negotiating success, more or less than the damage that follows blowback from allies offended by it (like Brazil, Germany, and others)?

-- Closely related is how much Snowden's revelations have helped or damaged liaison relations?

-- Blackmail, extortion and other crimes are also ancient tools of spies and secret power systems. How much has the massive increase in NSA (and "5 Eyes")[i] power increased the potential for manipulation of domestic political processes?

-- Closely related is how will police-states use these same technologies to better suppress critics in their own societies? How much did Snowden's revelations change that power of states, whether allegedly democratic or autocratic, to catch "terrorists" or suppress citizens they dislike?

-- Finally, how will the subsequent emphasis on "Insider Threats" affect quality of the entire US intelligence personnel corps? That is more practical and parochial than ethical and universal, but ethics affects who wants to be part of any large organization, and what caliber of people will put up with its constraints. Intelligence agencies worldwide have always worried about the loyalty of their employees and their agents (not the same people, technically) and since Snowden was an American IC (Intelligence Community) employee, his data dump prompted a vast search for more "insiders" who might be thinking about leaking secrets (a.k.a. whistleblowing).

These are at least eight big questions. We will do our best to answer them in the space available.

Introduction to the Biggest Questions:

What is more important, the Constitution or any Government Agency?

And does an 'Oath before God' mean more or less than a 'Contract with a Government'?

Every US Federal employee must swear an oath of allegiance to the US Constitution, including lowest ranking military and even employees of the Post Office (which is no longer technically a federal institution). The exact words vary from place to place and with rank, but the general theme is to "honor and support" or to "preserve, protect and defend" the US Constitution from all enemies foreign and domestic. Where security clearances are required for work, as in all 17 US intelligence agencies, an additional step is required, signing a formal "non-disclosure" agreement. Those agreements also vary with agency and rank, but they are more in the form of contracts where the signee accepts a responsibility to keep all secrets trusted to them from unauthorized people and especially from the press, under penalties of loss of job or security clearance, to loss of liberty in graver cases, and even to loss of life if convicted of violating the

Espionage Act of 1917 or the Sedition Act of 1918. Usually they are told about ways to legally (a.k.a. safely) question waste, fraud, abuse or outright criminal behavior in their institutions, like reporting to Offices of Inspectors General (IG) or to the House and Senate Intelligence Oversight Committees; sometimes they are not. Pity any employee who goes to the Congress regardless.[ii]

The central dilemma raised by Edward Snowden's disclosures is whether the Oath to the US Constitution trumps Contracts with Agencies, in his case the NSA, even though he was working for a contractor (Booz Allen) when he shared very large numbers of classified files with several press outlets for further vetting and release at their discretion. His complicated method of release highlights two points. 1) Mr. Snowden was very well aware of the dangers of releasing secret information, and of the importance of redacting particular bits like names of sources to protect them, so he wanted other professionals (from journalism not security) to share in his judgments on that.[iii] 2) He had zero confidence in the alleged protections of Oversight Committees and IG Offices, because he had seen how the US government treated other whistleblowers before him who had objected to the same kinds of practices, like Thomas Drake[iv] and William Binney[v] at NSA, who helped build the new technology architecture that enabled unprecedented intrusion into every citizen's private life, with or without judicial warrants as the Constitution calls for.[vi]

As a matter of law, this dilemma is a pivot point between true liberty and the perversions called police-states. Who is ultimately sovereign? The people, or security institutions? At least 800 years of jurisprudence starting with the Magna Carta signed by King John of England in 1215 CE have focused on the balance of power between governments (or kings) and people (or at least the very rich people called "barons" at that time). The rebellion of colonists in North America, and creation of the US Constitution in 1789 (amended 27 times, most recently on May 7, 1992)

was an especially important period for both thinking and written language on this topic. Those over 226 years of editing, are further edited every time the US Supreme Court publishes opinions on the actual meaning of words and ideas in the Constitution, like the importance of judicial warrants to search people's persons, property, records and effects, as required by Amendment 4.

In some constructions, 'ethics begins where the law ends.' Many current dilemmas stem from questions of information, and whether people have natural, legal or ethical rights to privacy in communications and/or personal data. That domain has been transformed by the revolution in information technology, which is why the government was hiring thousands of contractors like Edward Snowden to manage their new computers and powerful search and surveillance systems.

So whether you think the Constitution is the ultimate law in America, or contracts with agencies, is a non-trivial question. Of course, what we think is one thing, the Supreme Court is another.

How Have Such Disclosures Affected Practical Journalism?

Giving or receiving "classified" information has always been fraught with peril, for the giver who usually worked for some government, and for the receiver who was often a journalist. The US government (and many others) has a long record of overclassifying things that were merely embarrassing to someone in power, rather than integral to national security. Nothing covers "waste, fraud and abuse" better than the shield of secrecy, backed by penalties of law. Ask the Turks of Erdogan, or critics of Xi Jinping of China. Therefore, there is an equally long record of "investigative journalism" in America devoted to finding out what is really going on behind the

veils of secrecy. In the United States, this tradition depends heavily on another Amendment to the US Constitution, the first, respecting and protecting freedoms of speech and religion.

Long ago, this meant clandestine meetings between journalists and sources in seedy hotels or fancy restaurants (or in deserted parking ramps after secret signals as in the classic Watergate case[vii]). In those ancient times just 44 years ago, avoiding physical surveillance and telephones that could be tapped was usually enough to avoid detection and prosecution. The era of email, social media, bulk collections of telecom metadata and insider threat programs has transformed that. A determined signals intelligence agency like the NSA can now discover nearly everything about a "target" without ever getting near them or "tapping" their phone lines directly.

Combined with the most aggressive prosecutions of alleged "leakers" in the history of the American Republic by first the Bush-Cheney[viii] and then the Obama administrations,[ix x xi] this has greatly increased the peril of government insiders revealing secrets, and too often even of journalists who dare publish such information.[xii] One stunning result is that the most aggressive revealers of US secrets are now based overseas, like the Guardian (a British newspaper to which Snowden released his trove of documents) and the Intercept (a web based journal based in Brazil, created by American journalists, Glenn Greenwald and Laura Poitras, to whom Snowden also released his documents stolen from NSA). A documentary about that complex process worth watching is "Citizenfour" produced by Poitras in 2014. It features Snowden talking directly about his reasons for disclosure, Greenwald about publishing some of the resulting stories, and William Binney[xiii] who helped create the NSA surveillance system before resigning in Oct. 2001.

So, the ability of journalists to successfully investigate crimes by secret agencies in the USA has undoubtedly declined during this time. And risks to government whistleblowers have increased dramatically. More on this is covered in the section on "Insider Threats" to follow.

Whether this is good or bad depends fundamentally on whether you think ultimate sovereign power resides with the people, or with any government. If your primary loyalty is to the people, whistleblowers are heroes. If you prefer the government, they are leakers at best and traitors at worst. The US Constitution was created specifically to address this tension of sovereignties.

Disclosures Enhance Accountability, but do they Damage Legitimate Defense More?

An accurate answer to this question would require a God-like vision of things that are difficult for anyone to measure. What is certain is that "perfect" accountability would require complete transparency, which no intelligence agency could endure. And "perfect" defense prefers absolute secrecy, with the inevitable corollary of impunity for those who commit willful crimes, or just make mistakes during secret operations. These are opposite imperatives, so a better question might be, "How can a free society find the best balance between liberty and security?"

One of our founding fathers, Benjamin Franklin, said this about that: *"Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety."* And one of the best critics of the rush by US intelligence agencies to know everything about everyone (Bruce Schneier) points out why true freedom requires some privacy, and that with computers the tradeoff metaphor may be inaccurate. He maintains that real security lies in knowing what is

going on rather than in keeping secrets on the government side, and in durable privacy rights for citizens. Schneier concludes that both freedom AND security are enhanced by strong encryption and limits on allowable government searches and seizures, as called for in our Constitution.[xiv]

Bradley Manning[xv] signed up with the Army after 9/11 and was a private in military intelligence when he began to be disturbed by what he saw in the classified traffic on Iraq that crossed his desk. He thought war crimes were being committed, and eventually that the whole premise of the US invasion of March 19, 2003 was a lie. A very big lie.[xvi] Suffering a severe crisis of conscience after years passed with no evidence of the alleged Weapons of Mass Destruction used as a pretext for this invasion, Manning smuggled out a load of secret documents in April of 2010 and gave many to a relatively new internet organization called "WikiLeaks" (based in Iceland) that specialized in handling classified documents that exposed official wrongdoing.[xvii] One of those got dramatic international attention, video taken from an Apache helicopter of a dozen civilians being killed in Iraq on July 12, 2007. They included two Reuter's photographers whose cameras were thought to be possibly weapons. The term "Collateral Murder" became a label for this video and several versions are viewable on YouTube today.[xviii] A rescue van called in by one of the wounded arrived minutes later and was also attacked, killing more civilians and wounding two children in the van. That did not fit well with the public relations version of the war in Iraq.

Disclosures like this reveal at least the brutality of modern war, which is the main reason why the US Pentagon no longer allows uncensored reporting from combat zones today, unlike in Vietnam where media revealed many unpleasant truths to the American public that led eventually to a

negotiated end to that war. We lost, which is not a goal of any military. Even worse, from their point of view, uncensored reporting can reveal lies used to justify the war itself. And it can reveal war crimes, which no institution wants to expose its employees to prosecution for.

Men like Edward Snowden undoubtedly paid attention to what happened to whistleblowers before them like Bradley Manning, Thomas Drake and others. So when Snowden did his data dump, he went large scale, and used a very elaborate process to get very large quantities of data out focused on the explosive growth of electronic surveillance during that time. He also watched then NSA Director Gen. Keith Alexander, and then Director of National Intelligence Gen. James Clapper lie to Congressional Oversight Committees about the extent of such surveillance of US citizens after direct and well-focused questions by committee member Ron Wyden (a Senator). So Snowden knew that the "oversight" process was at the least very compromised.[xix]

How much did those disclosures damage "legitimate self-defense?" This question hinges on definitions of "legitimate." Were these wars morally defensible, there would have been few crises of conscience among both soldiers and intelligence personnel waging them. There is a long history of US reporters and media institutions cooperating extensively with both Pentagon and intelligence agencies to protect sources, methods, and operational details that could result in terrible loss to our troops or our agents if revealed to public eyes. With very rare exception, whistleblowers only emerge when crimes are egregious, large, and persistent.

Mass Surveillance can provide Diplomatic Leverage and Battlefield Advantages, but it also causes blowback among allies and citizens and damages liaison relations. Which is greater?

Apple Corporation was recently locked in battle with the FBI over demands they write new code to create a "backdoor" into secure, encrypted iPhones. The lead editorial of the Feb. 19, 2016 Wall Street Journal gives a balanced and carefully fact-checked review of many dimensions of that case. [xx] The only part they neglect is the pervasive effect of what spies call "blowback." That happens when your own citizens are adversely affected by security operations, and when targets realize they are being targeted. Resistance is expected when the targets are enemies. But blowback goes ballistic when the targets are your own citizens or your allies.

Brought up on principles of freedom, US citizens respond poorly when their money is used to undercut liberty by funding weapons of war (which security intelligence certainly is) that target them. The biggest downside of Snowden's revelations was showing how casually the NSA had decided to surveil almost every phone call every American makes, and then lied about that to oversight committees of Congress. The NSA also used its shiny new powers to target friendly institutions like the United Nations[xxi] and close allies, like Brazil, Israel, Italy and Germany, and even German Prime Minister Angela Merkel's personal cell phone.[xxii]

Brazilian President Dilma Rouseff's speech to the UN about that calls for cold drinks to chill her spicy language.[xxiii] And one of our most important allies in Europe ordered an overhaul of liaison relations with America after Snowden showed that we were not just gathering metadata, but actually recording personal communications of the Prime Minister and other key officials.[xxiv]

This has vast commercial consequences far beyond the security consequences of angering allies and compromising critical liaison relationships among intelligence and military bureaucracies.

Among Snowden's many other revelations was how thoroughly the NSA and its top ally in such endeavors, Britain's GCHQ, had compromised commercial entities like the telecom companies and big internet companies like Apple and Google, Facebook, Yahoo, Twitter, etc. A paradigm became clear.[xxv] First the intelligence agencies asked politely if companies would simply give them all their customer's data. Then, if that failed, the agencies offered to buy the data. Then, if that failed, the agencies often chose to steal the data by tapping into the server farms and internet backbones that everyone uses to move big data around these days. Give, buy, steal: a paradigm!

Many companies are considering moving data onto less expensive servers controlled by other companies, like Apple, Google and a hundred international competitors, commonly called the "cloud." But now they know that if you give your data to a US firm, you probably have given it to the US government as well! This is a trillion dollar disadvantage for companies that make their living by proprietary information. So having learned about this, many are simply refusing to patronize US technology companies, and secure encryption has become an industry standard.

Tapping telephones at the UN has also undoubtedly provided diplomatic advantages from time to time, and intercepting enemy communications has undoubtedly won some wars.[xxvi] So good signals intelligence can certainly provide battlefield advantages, and diplomatic leverage from time to time. A recent NSA Director, General Michael Hayden (in response to questions about metadata) even famously said one day that "We kill people based on metadata".[xxvii] What they actually do is to send Hellfire or other missiles to home in on selected cell phones, chosen by metadata filtering, and hope that the phone is being held by the man they actually want to kill.

Practical experience shows that the answer to that is sometimes yes, and sometimes no. This is why it is standard practice to TRY to verify that the targeted phone is actually in possession of the intended human target, and that the phone is not near a school, mosque or other site where many innocent victims would also be injured or killed. The US military tries very hard to do that, to avoid collateral damage (killing innocents) when they "can" although videos like collateral murder show that this is not always, well, accurate. The CIA – you better ask them, because they pretend that all their targets are very evil enemies even though their Phoenix program in Vietnam showed graphically how sloppy that can be in the fog of real wars.[xxviii]

We have lost allies all over the world by "collateral damage" (killing innocents) even though everyone recognizes that perfection is not possible in modern armed combat. This negative blowback effect is increased when intelligence agencies choose to target everyone on the theory that needles need haystacks and that everyone is a legitimate suspect in the global war on 'terror.'

Snowden revealed more than any other the vast extent of that intrusion by modern signals and technical intelligence. The commercial world is still adapting to consequences. Everyone knows, for example, that the Chinese are very aggressive at collecting economically useful information including manufacturing and information technologies through espionage. And many hate them deeply therefore. We are on the lip of suffering similar economic costs to big American companies like Apple and Google because of cooperation (voluntary and compelled) with US intelligence agencies that compromises promises of data security for their customers.

The last word on damage to liaison relationships is this. Our allies have not been offended by Snowden's revelations (excepting perhaps Britain's GCHQ which was revealed to be such a poodle for the NSA). Allies like Germany, Brazil and dozens of others were offended by the behavior of the NSA and US government. Blaming sins on the messenger who reveals them is an ancient vice of spies and princes, but this is mere evasion of responsibility for Agency acts.

Mass Surveillance, especially Bulk Metadata and "Big Data" Collection, provides vast potential for Blackmail, Extortion and other dark and ancient tools of espionage tradecraft. Can 'Oversight' mechanisms actually prevent that? Really! How?

J. Edgar Hoover, 48 years director of our FBI and its preceding Bureau of Investigation, secured his power partly by developing compromise files on every politician he could. These held embarrassing information that could be used if any looked too closely at the FBI. It was seldom necessary to leak such information. Rather the clever Director would just invite the target in to show them damaging information that the agency had 'become aware of' which would be 'carefully guarded' by the FBI in the best interest of the politician. Most politicians were bright enough to recognize what that actually meant, and chose to exercise their curiosity elsewhere.

Hoover did not have anything like the surveillance capabilities that the NSA deploys today. But he was probably the most feared and hated FBI Director ever, which exemplifies the systemic dangers of secret and unaccountable power.[xxix]

Hoover had enough HUMINT to use psychological operations techniques against peace activists, labor organizers, and most memorably the Rev. Martin Luther King, starting one month after John F. Kennedy's murder and ending with King's death five years later. This infamous period in FBI history is known as the COINTELPRO program,[xxx] and it had many targets much less famous than Dr. King. The 1976 Church Commission that investigated profound wrongdoings among the US intelligence community accused Hoover and the FBI of using illegal and often unconstitutional methods in their zeal to catch and disrupt, or even to destroy any possible 'subversives.' Any critic of government was liable to be called a communist in those days (and investigated) or worse, a traitor (then imprisoned or killed if convicted). Imagine Hoover, or men like him, with modern SIGINT capabilities and a shield of secrecy amounting to impunity.

Bulk metadata collection is presented as benign because it does not automatically provide the content of communications. But it does provide an almost unlimited potential for searching for links between phones owned by power people with phones used by brothels, organized crime figures, terrorists, or foreign governments and alleged agents for them. You do not need to know any content of such communications to draw negative inferences from such associations.

Friends of mine from the CIA taught me a phrase called "the fine art of human compromise." Friends from law enforcement taught me about varieties of sexual blackmail, including use of juveniles for people vulnerable to that. Hoover aside, all should know that the classic toolkit of espionage called "tradecraft" has always included bribery, blackmail, extortion, assassination and threats of assassination. Such tactics can cause a foreign official to reveal secrets even when they do not want to. Bribery, or simply buying secrets, or putting officials on undercover payroll

(a fact that can always be revealed to enemy law enforcement if necessary, turning bribery into extortion) are by far the most common. But all of these are tools that real spies sometimes use.

Imagine modern case officers with the power of metadata collection of EVERYONE in a target country. This is a great temptation to actual spies whatever their particular rules of conduct.

Do spies lie? Do birds fly? Do spies break rules? Warn the children: spy agencies have schools to teach agents how to break the rules of other countries routinely and escape, usually unharmed. Some spy agencies actively recruit for high-level psychopaths, because they make better spies (if they can be controlled, which is an ever present problem with true psychopaths). Because of these very unusual conditions, backed by special laws that exempt "intelligence professionals" from some of the constraints of law applied to others, have led to the birth of a very weak subfield called intelligence ethics [xxxi], [xxxii], [xxxiii]. A small international society was even created to promote that (International Society for Intelligence Ethics) which held several conferences and created a journal. But it faced opposition from much of America's IC which was, to be blunt, afraid of both genuine ethics and effective oversight. One of the IIEA's journal issues was devoted specifically to that topic [xxxiv] before both journal and society essentially disappeared.

Well, oversight exists in theory to prevent such kinds of overreach by official spy agencies or agents. That 'oversight is often compromised' is a huge understatement. The first politicians a really wicked spy agency tries to compromise are those on oversight committees, and it does not take many to cripple the whole enterprise due to the shield of secrecy and functional impunity that keeps honest politicians from reporting directly and accurately on crimes they discover.

The history of CIA torture manuals and practices, from its OSS origins,[xxxv] to the MKULTRA program of the 1960's,[xxxvi] to "KUBARK"[xxxvii] and "Operation Phoenix" during the Vietnam War period[xxxviii] to "Psychological Operations in Guerilla Warfare" in 1983 Nicaragua,[xxxix] to the scandals of Abu Ghraib in Iraq,[xl] waterboarding, and beating people to death in other countries (see "Taxi to the Dark Side"[xli]) as documented in the Senate Intelligence Committee's Torture Report [xlii] (90% of which is still kept secret from citizens by the corrupt classification system) proves that whatever "oversight" exists is at the very least *thoroughly* compromised.[xliii] This sequence also illustrates how slowly secret systems learn the downside of practices like torture.

So we encourage the reader just to contemplate whether the stunning new powers of surveillance revealed by Edward Snowden would a) increase, or b) decrease the possibility of their domestic use by the kinds of people employed to break every law of god and man against other countries.

Then we encourage all to consider how police-states are likely to use such power, unencumbered by civil libertarians and concerns about human rights, personal freedom or other quaint concepts.

How will Police-States use these same powers to Suppress Dissent in their Countries? Have Snowden's revelations increased or decreased those dangers?

Police-states will continue to do what they have always done, which is to use every power at their disposal to detect and suppress dissent within their countries. In fact a diagnostic difference between police-state intelligence services and idealized democratic ones is whether they target domestic dissent, or not. The new powers of modern information technology revealed by

Edward Snowden, but created by the NSA and other entities with "the best of intentions," will be used, and are being used today, to crush liberty and diminish hope in police-state countries. The FBI can now turn on your smart phone secretly to record whomever you are talking to today, and to download your contacts and emails surreptitiously; tomorrow North Korea will be able to also.

Russia and China suppress dissent ever more effectively as tracking their targets and discovering their networks of connections becomes easier. Turkey and Egypt, once hopes for enlightened Islam, digress as their leaders go down the dark tunnel marked "power corrupts." The Arab Spring was crushed as journalists eager for a little more freedom discovered that things can change overnight, and that liberty is very perishable. Propaganda potentials have barely begun to be expressed. North Korea remains the living hell it was before, while Saudi Arabia and Iran compete for the title of world's leader in executing alleged enemies of the state. Some, like Sheikh Nimr Baqir al-Nimr, were simply seeking justice for their peoples using Martin Luther King-type non-violent techniques. Nimr was beheaded on January 2, 2016, for calling for free elections in Saudi Arabia and preaching about human rights for the Shia Minority there.

Thank God none of these countries own the backbone of the internet like America does today. That dominance too shall pass as the world reacts to vulnerabilities revealed by Mr. Snowden. Possibly the biggest loss to America has been our strategic goal of promoting "rule of law." To do that one needs moral standing. No one believes the USA anymore, since they have seen how casually our government violated international agreements to respect the privacy of diplomatic conversations at the UN and even among very close allies. They have seen how casually we lie about our wars. All because the USA is terrified by terrorists. Even domestic unity declines as

our government shows that the formerly sacrosanct US Constitution is far less potent today than rules of secret bureaucracies, at least when it comes to freedom of speech and association.

Surveillance <u>within</u> US Intelligence (and military) Agencies has become much stricter now due to Snowden's Revelations. Does this "Insider Threat" program enhance or degrade the overall quality of personnel who will join and work for intelligence agencies?

One undeniable consequence of Snowden's revelations (and other whistleblowers') is increased emphasis in America's IC (intelligence community) on trying to detect employees who <u>might</u> reveal secrets before they do, whether from crises of conscience or crass ambitions for money, fame, revenge or whatever. Reasons why seldom matter to counterintelligence personnel who are focused on keeping the secrets, and with no exceptions known to me consider non-disclosure contracts to supersede oaths to support or defend the Constitution. Those I know say and believe they are defending the Constitution by keeping secrets from citizens, since anyone <u>might</u> be a spy. One modern bureaucratic expression of that goal is called the "Insider Threat" program.[xliv] This was established on October 7, 2011 by President Obama's Executive Order 13587.[xlv]

There are precedents. Those familiar with the CIA remember the famously paranoid 20 year Director of Counterintelligence at CIA named James Jesus Angleton. Angleton's zest for finding possible "moles" (enemy spies) within that agency resulted in measures like mandatory and now periodic exams with "lie detectors" despite many known flaws in that equipment and subjective polygraph operators who sometimes seem more interested in sexual topics than in operational conduct. The agency was riven with suspicion during this period, driven by both valid concerns about communist penetration, and arguably paranoid concerns enhanced by alcohol, which many

agreed was a growing problem toward the end of Angleton's tenure. This is another unintended but sadly real byproduct of intensive surveillance and hyper-detailed rules of personal conduct. Former DCI Admiral Stansfield Turner found that the CIA had the highest rates of alcoholism and divorce of any US government agency in the late 1970's, or so he told me personally.

Another, later expression of this priority of secrecy over Constitutional liberty was President Obama's unprecedented effort to prosecute leakers from the intelligence community under the 1917 Espionage Act.[xlvi] That is distinguished from modern laws by featuring the death penalty, which certainly puts more fear into employees with security clearances. Even accidental exposure, like losing a flash drive, or leaving a laptop in a taxi or a car that is then stolen can be cause for discipline, dismissal or, in fact, death if the motive is deemed to be treason.

Another unintended consequence is progressive decline in the quality of the workforce all intelligence agencies depend on. Why? Because "best qualified" people will only put up with so much intrusion into private lives, background checks, surveillance, polygraph exams, etc. Many "best qualified" people do not want to submit their sex lives to strangers, or everything they write about serious topics for the rest of their lives to review and censorship by agencies and often anonymous security officers. Some do not want to report every non-US citizen they correspond with, for permission to continue. Many would like to marry without running their spouse through security for a "background check." The Insider Threat program infringes ever more on what most consider normal freedoms of citizens in true democracies. So <u>many</u> better people leave the IC early, and others never apply to work there. Some read the memoirs of former career officials embittered by their encounters with mindless bureaucracies and bone-headed security officers whose main ticket in life is the power to say "no" to cleared intelligence

personnel. One significant effect of this is reduction in the quality of people employed by such agencies. Another is mental illness, but that is a larger and very delicate topic. Most arrive intact and with excellent intentions, but they enter an environment that is toxic to mental health. Secrecy inhibits wisdom, hubris corrupts it, pressures are vast, and the inability to consult with trusted others is actually dangerous when stresses of their very difficult jobs becomes too great.

IC human resource departments are sometimes quick to point out how many applicants agencies get and reject each year, for well-paid jobs with excellent benefits. But that is quantity. IC-HR departments do not generally release quality measures. One reason why is because such data can be embarrassing, sometimes disturbing, and often is contrary to bureaucratic party lines.

I mean no disrespect to those who choose to serve their country despite such onerous restrictions on their lives, and thus endure the waste required to satisfy the security gremlins. But I must point out how obsessions with secrecy and surveillance damage both freedom and true security. Aristotle noted that real virtue lies between extremes, and that any virtue taken to extremes can become a dangerous vice.[xlvii] The balance between liberty and secrecy has serious consequences for intelligence professionals and their families, as well as for the countries they work for.

There are very legitimate roles for secrecy and surveillance in national security intelligence. But obsession with those goals is damaging America and the world today. The problems I describe are not at all confined to the USA, but they tend to be more visible because the US is more transparent than many countries. To solve this problem, agencies must move beyond public relations and crafted rationalizations to be honest with the publics that fund and empower them. Then they must restrain their excesses. Or, publics need to radically reform offending agencies

to honor our oaths to preserve and defend our Constitution in the USA, or to protect the people during times of danger anywhere. That is the original, noble mission of good spies worldwide.

Conclusions

Edward Snowden revealed that, with the best of intentions to catch "terrorists" and shielded by excessive secrecy, the NSA had created a signals intelligence system that any police-state would envy. It is now capable of monitoring the great majority of all telecom and internet activity of most American citizens, and many non-US people, and routinely does so. Then, when challenged on this by oversight committees of Congress, senior officers lied. So Snowden revealed a large number of very inconvenient truths to both our public and to the world. Those truths challenged the ethics of the agencies involved far more than their technical proficiency or nominal goals.

Perhaps the dumbest thing the US did when it discovered Edward Snowden's revelations was to force him to stay in the Moscow airport for days on his way to Ecuador, by yanking his passport when what the agencies really wanted to do was arrest or abduct him. Vladimir Putin promptly offered Snowden asylum, and lacking options he now lives in Russia where his exceptional talents and insider knowledge must contribute in some way to their maneuvers against the west.

He would have cheerfully come home if offered immunity, to discuss the problems he exposed. That was his often expressed goal, to generate discussion about civil liberties in surveillance states. Snowden's revelations have shown the world how immoral bureaucracies can become, even when they are staffed by patriotic human beings with consciences (mostly) motivated by the best of intentions. But bureaucracies care about money not morality.[xlviii] His revelations

provide an early warning of grave dangers to freedom in particular, to peace, and even to the existence of the republic. In the very worst case scenarios, this endangers human civilization itself, because police-states inevitably degenerate, and many have nuclear weapons today.

Having created this monster of police-state surveillance of everyone all the time, at great cost to the republic and indifferent to quaint concepts like "probable cause" or "freedom and liberty," administrators then rationalized how this might be good for ordinary people. The distortions of law and truth that resulted are tragic because they express respect for the ancient virtues while garroting and burying the real meaning of things like freedom, justice and rule of law. Party line lawyers did that to the word "torture" and look where that got America.[xlix] That is the greatest corruption of all, when the very meaning of critical terms like freedom, rule of law, justice and torture become distorted or inverted by rationalizations created to enhance someone's budgets.

Therefore, those who wish to solve such problems must confront four inconvenient truths.

1. Bureaucracies are NOT people; they do not have intrinsic consciences, but they do act on the world in Darwinian ways, because like any living system they compete with others for critical resources. Intelligence bureaucracies exclude people who won't keep secrets.
2. Intelligence bureaucracies are dangerous in particular because they insist upon shields of secrecy behind which evil can thrive. Their goals are nominally good, like the soldier who faces danger to protect his or her society. But if they were always truly good they would not have such deep, compelling and compulsive needs for secrecy.
3. Such environments are especially attractive to psychopathic personalities who also lack conscience, are driven by lust for power, and enjoy significant advantages against gentler people in competitions for secret power. This is why some intelligence agencies actively

select for psychopaths on their operational side (analysts are less damaged, but almost never rise to the top to dominate operators). Others (e.g. the French) are well aware of the dangers of psychopaths, and work hard to exclude them from their intelligence systems.

4. Intelligence bureaucracies also learn slowly, partly because they reject critics and punish ethical employees. In fact, they often label such people national security threats, because they refuse to keep crimes secret. Such people are usually just threats to the bureaucracy. Therefore, reform of intelligence systems is essential for healthy democracies to survive.

These are my opinions on the ethical implications of the Snowden revelations. What you do about those problems is up to you, but I conclude by paraphrasing Franklin. It is an honor and a duty to protect both our peoples and the freedoms they cherish. But those who would sacrifice freedom for a little temporary safety or tactical advantage deserve neither freedom nor security, and will harvest a "Legacy of Ashes." [1] If professionals do not seek the proper balance, publics eventually do, which is why police-states always fall in the long run of human civilizations.

References Cited:

Ackerman, S. and Ed Pilkington (2015, March 16). Obama's War on Whistleblowers Leaves Administration Insiders Unscathed, London, UK: *The Guardian.*

Andregg, M. (2007). *Intelligence Ethics: The Definitive Work of 2007**, St. Paul, MN: Ground Zero MN.

Aristotle. (~ 350 BCE) *Nichomachean Ethics,* pp. 42, 1107a, lines 1-5 of book 2, chapter vi.

Bamford, J. (2012, March 15). The NSA is Building the Country's Biggest Spy Center (Watch What You Say), *Wired.*

Bamford, J. (2005). *A Pretext for War: 9/11, Iraq, and the Abuse of America's Intelligence Agencies*, New York, NY: Random House.

Borger, J. (2013, September 24). Brazilian President: US Surveillance a 'Breach of International Law', *The Guardian* (London, UK).

Calderon, Michael and Matt Sledge (2013, April 16). Obama Whistleblower Prosecutions Lead to Chilling Effect on Press, *Huffington Post*.

CBS News, (2011, May 22) *60 Minutes*. "U.S. vs. Whistleblower Tom Drake."

CIA, "Tayacan" (1985). *Psychological Operations in Guerilla Warfare*.

CIA, "KUBARK" (1963, July). *KUBARK Counterintelligence Interrogation*.

"Collateral Murder", a video record of events in Iraq on June 12, 2007 can be seen at: https://www.youtube.com/watch?v=5rXPrfnU3G0 .

Colby, W. and Peter Forbath. (1978). *Honorable Men: My Life in the CIA*, New York, NY: Simon and Schuster.

Cole, D. (2014, May 10). We Kill People Based on Metadata, *The New York Review of Books.*

Cole, D. (2009, October 8). The Torture Memos: the case against the lawyers, *The New York Review of Books.*

Der Spiegel (2013, October 28). Embassy Espionage: The NSA's Secret Spy Hub in Berlin, *Spiegel Online English.* Original published as "Das Nest" in *Der Spiegel.*

Feinstein, Dianne (2014). US Senate Intelligence Committee Report on Torture: Committee Study of the Central Intelligence Agency's Detention and Interrogation Programs.

Frontline, (2013). United States of Secrets, *PBS.*

Gibbons, Chip (2016, March 5). How the FBI Polices Dissent and Why it Matters in the Encryption Debate, *Truthout.*

Gibney, A. (2007). *Taxi to the Dark Side.*

Goldman, J. (2006). *Ethics of Spying: A Reader for Intelligence Professionals.* Lanham, MD: Scarecrow Press.

Goldman, J. (2012) ed. *International Journal of Intelligence Ethics,* Vol. 3, No. 2, Fall/Winter.

Greenberg, J. (2014, January 10). CNN's Tapper: Obama has used Espionage Act more than all previous administrations, *politifact.com.*

Hager, N. (1996). *Secret Power: New Zealand's Role in the International Spy Network.* Nelson, New Zealand: Craig Potton Publishing.

Hummel, R.P. (2015). *Understanding Bureaucracy*, (especially Chapter 3 on the Psychology of Bureaucracies, pp. 123-160. University of Texas, Austin

Lewy, Guenter (1978). *America in Vietnam,* London, UK: Oxford University Press.

Olson, J. (2006). *Fair Play: The Moral Dilemmas of Spying,* Washington, D.C.: Potomac Books.

Omang, J. and Aryeh, Neier (1985). *Psychological Operations in Guerilla Warfare: The CIA's Nicaragua Manuel,* New York, NY: Vintage Books.

Poitras, Laura (2014). *Citizenfour*.

Rich, F. (2006), *The Greatest Story Ever Sold: The Decline of Truth in Bush's America*. New York, NY: Penguin Books.

Risen, James (2006). *State of War: The Secret History of the CIA and the Bush Administration,* New York, NY: Free Press.

Risen, James (2014). *Pay Any Price: Greed, Power and Endless War,* New York, NY: Houghton Mifflin Harcourt.

Schneier, B. (2015). *Data and Goliath: The hidden battles to collect your data and control your world.* New York, NY: W.W. Norton & Company.

Shanker, S. (2016, February 23). WikiLeaks Says US Spied on Meetings of UN Chief, Angela Merkel, Benjamin Netanyahu, *International Business Times.*

Strasser, S. (2004). *The Abu Ghraib Investigations: The Official Reports of the Independent Panel and the Pentagon on the Shocking Prisoner Abuse in Iraq*, New York, NY: Public Affairs LLC.

United States Senate (1977, August 8). Project MKUltra, the Central Intelligence Agency's Program of Research into Behavioral Modification. Joint Hearing before the Select Committee on Intelligence and the Subcommittee on Health and Scientific Research.

Wall Street Journal (2016, February 19). *The FBI vs. Apple*, lead editorial.

Weiner, T. (2008). *Legacy of Ashes*, New York, NY: Anchor Publishing.

Wilson, V.P. (2008). *Fair Game: How a Top CIA Agent was Betrayed by Her Own Government*, New York, NY: Publisher.

Woodward, B. and Carl Bernstein (1974). *All the President's Men,* New York, NY: Simon and Schuster.

---

[i] "5 Eyes" is signals intelligence trade jargon for an alliance among the intelligence systems of the USA, UK, Canada, Australia and New Zealand who have been sharing communications intercept data for many decades. This alliance has become ever more important as signals intelligence has grown to include computer data. A good reference on that and on the Echelon system which scanned international telecommunications for keywords is Hager, N. (1996). *Secret Power: New Zealand's role in the international spy network.* Nelson, New Zealand: Craig Potton Publishing. That was 20 years ago; the technology and infrastructure of state surveillance has come a LONG way since then.

[ii] The case of FBI whistleblower Coleen Rowley is instructive here. A career FBI attorney, she sent a 13 page analysis to Director Robert S. Mueller about problems assessing intelligence prior to 9/11 that arguably allowed that attack to proceed by ignoring warnings two months prior by agents in the field. When those in-house channels failed to produce any constructive outcomes, she eventually and reluctantly shared her letter to Mueller with Congressional Oversight Committees. Rowley was named one of three "persons of the year" by Time Magazine in 2002, all of whom were female whistleblowers. Therefore she was ostracized by her agency, even though they dared not fire her directly. She retired early a few years later, but became expert on the many ways by which bureaucracies can retaliate against those who reveal embarrassing information even if they do not reveal any classified information.

[iii] Laura Poitras was producer and director of *Citizenfour*, a video documentary produced in 2014 featuring Edward Snowden, Glenn Greenwald (one of the reporters that Snowden released his stolen files to) and William Binney (one of the NSA veterans who resigned when he saw how modern technology that he helped create to protect America was being used to undermine US civil liberties and arguably the US Constitution itself). It won the 2015 Academy Award for Best Documentary.

[iv] CBS News' *60 minutes* did a lengthy piece on the persecution of NSA veteran Thomas Drake called "U.S. vs. Whistleblower Tom Drake" that aired on May 22, 2011, accessible at: http://www.cbsnews.com/videos/u-s-v-whistleblower-tom-drake/. Drake was a senior executive at NSA and a decorated Air force and Navy veteran who objected to replacing an NSA produced, civil liberties protecting, "Thinthread" system with a billion dollar plus, contracted system that neither protected US civil liberties nor did much of any good finding "terrorists" which was the original justification for creating these metadata software programs. Drake never went to jail when charges were dropped after their idiocy was exposed by 60 Minutes, but four years of defending himself destroyed his career and personal finances, which is enough to send signals to anyone else inside the classified cocoons who thinks about objecting to "waste, fraud and abuse" even through official channels. This was the remarkable thing about Drake; he did not go to the press prior, and he never revealed any classified information to anyone. Rather Thomas Drake sent his objections through official and secret channels until they indicted him anyway.

[v] Bamford, J. (2012, March 15). The NSA is Building the Country's Biggest Spy Center (Watch What You Say), in *Wired*, at: http://www.wired.com/2012/03/ff_nsadatacenter/. James Bamford wrote 3 classic books on the NSA in 1982, 2001 and 2008, and was invited to the NSA for book signings when they were less allergic to disclosure of aggressive surveillance of all US citizens who use telephones, cell phones, or the internet as they are today in 2016. Such data are now stored at the Bluffdale storage center in Utah which Bamford was writing about for Wired.

[vi] The Fourth Amendment to the US Constitution, part of what is commonly called the "Bill of Rights," deserves explication here, because it contains many key words that have become fundamental to American jurisprudence, like "probable cause" and "warrants." This has prompted a long list of objections by intelligence agencies more interested in their security missions and budgets than with civil liberties. This ancient aspect of government priorities is why the Bill of Rights was adopted, for explicit protection of rights of individuals faced with state powers, which always include force as a last resort, as in arrest, jail or even death. In full, this Amendment reads: *"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."*

[vii] Woodward, B. and Carl Bernstein (1974). *All the President's Men*, New York, NY: Simon and Schuster.

[viii] Passed by Congress and signed by President George W. Bush in a very big rush after "9/11" on October 26, 2001, the USA PATRIOT Act authorized far more intrusive and aggressive surveillance of American citizens and "US Persons" (a technical word of great importance to the government in this context) than ever before in American history. Aggressive surveillance of persons outside of the United States may or may not have been illegal under the laws of those countries (usually illegal) but aggressive surveillance of US citizens had been prohibited without judicial warrants and probable cause to believe that crimes had occurred or were being planned. An official description of the Patriot Act and its later modifications can be found at the US Department of Justice, at: http://www.justice.gov/archive/ll/highlights.htm .

[ix] Greenberg, J. (2014, January 10). "CNN's Tapper: Obama has used Espionage Act more than all previous administrations," cited on politifact.com, and accessible at: http://www.politifact.com/punditfact/statements/2014/jan/10/jake-tapper/cnns-tapper-obama-has-used-espionage-act-more-all-/

[x] Washington's Blog (2015, May 11) Obama has sentenced Whistleblowers to 31 times the Jail Time of All Prior U.S. Presidents COMBINED, accessible at: http://www.washingtonsblog.com/2015/05/obama-has-sentenced-whistleblowers-to-31-times-the-jail-time-of-all-prior-u-s-presidents-combined.html

[xi] Calderone, Michael and Matt Sledge (2013, April 16). Obama Whistleblower Prosecutions Lead to Chilling Effect on Press, in the *Huffington Post*, accessible at: http://www.huffingtonpost.com/2013/04/16/obama-whistleblower-prosecutions-press_n_3091137.html

[xii] For example, James Risen of the *New York Times* faced a seven-year legal battle to defend his right to protect the identity of sources he used to acquire and then publish information in a book about manipulations of intelligence information in order to "sell" the US invasion of Iraq in 2003, called *State of War: The Secret History of the CIA and the Bush Administration* (Free Press, 2006). Under threat of prosecution by the Justice Department, Risen decided to use those years to write a follow-up book titled: *Pay Any Price: Greed, Power and Endless War* (Houghton Mifflin Harcourt, 2014). He prevailed, but most journalists do not have Pulitzer Prize reputations and the legal staff of the New York Times to help them fight the power of governments to prosecute journalists. His alleged source ultimately did go to jail for allegedly confirming some activities of the CIA against Iran, but Risen did not help them.

[xiii] In 2012, William Binney pinched his fingers and said "We are, like, that far from a turnkey totalitarian state." This quote can be found in James Bamford's security column for *Wired*, March 15, 2012, "The NSA is Building the Country's Biggest Spy Center (Watch What You Say)." Binney further described his reasons for resigning from the NSA after 36 years and helping to create the most scary internal surveillance technology ever invented because NSA refused his recommendations for protection of civil liberties. These comments occur in a 2013 *Frontline* Documentary, United States of Secrets, accessible at: http://www.pbs.org/wgbh/pages/frontline/government-elections-politics/united-states-of-secrets/the-frontline-interview-william-binney/ .

[xiv] Schneier, B. (2015). *Data and Goliath: The hidden battles to collect your data and control your world*. New York, NY: W.W. Norton & Company.

[xv] Now called Chelsey Manning because s/he has sought sex change treatments while serving her 35 year sentence in Ft. Leavenworth military prison. That is a digression irrelevant to the problems discussed in this paper. It does bear notice that none of the soldiers who murdered the civilians and Reuter's reporters in Iraq has been disciplined in any known way. But Manning serves a 35 year sentence in a military prison for revealing that truth to the American public that hired and armed the soldiers, and which in theory is responsible for every aspect of that war.

[xvi] Which turned out to be correct. See Bamford, J. (2005) *A Pretext for War: 9/11, Iraq and the Abuse of America's Intelligence Agencies*; Rich, F. (2006) *The Greatest Story Ever Sold: The Decline of Truth in Bush's America*; and Wilson, V.P. (2008) *Fair Game: How a Top CIA Agent was Betrayed by Her Own Government* for details about that big lie and its huge consequences (~$2 trillion wasted killing something like a million people).

[xvii] WikiLeaks was created in Iceland because protections of press freedom there are now greater than in the USA or Britain, which still think themselves as bastions of free speech, but are clearly no longer leaders in that domain. Iceland is undoubtedly much more free today in many ways than the USA which proclaims itself "the land of the free and the brave" at virtually every sporting event. For another example, consider the fact that Iceland jailed its bankers who committed crimes that contributed to the global "Great Recession" rather than "bailing them out." Iceland therefore recovered much faster economically than either the USA or the EU.

[xviii] The most watched version of "Collateral Murder," with context edited in text and a full 17 minute video version of events rather than compressed can be seen at: https://www.youtube.com/watch?v=5rXPrfnU3G0

[xix] In the words of my Congressman to me, those oversight committees were designed to "overlook" rather than to oversee, and a Senator who had been Chairman of the Senate Intelligence Oversight Committee also warned me personally on lengths the spooks would go to suppress truth; I quote: "When those guys get upset, there are real consequences." He would end up losing his Senate seat because he revealed too much truth about a secret war.

[xx] "The FBI vs. Apple" (2016, February 19) in *The Wall Street Journal*, lead editorial.

[xxi] Bugging selected UN phones was of course common long before new technologies made it almost routine. The difference between then and now was the cost in money, time and diplomatic risk. Today it is so easy and cheap to tap lines remotely that the NSA has taken the approach of "collecting everything" just because they can, as encouraged by then NSA Director Keith Alexander and revealed by Edward Snowden. This indifference to both domestic laws and informal but important international diplomatic protocols led to the rapid growth of their now global surveillance system that is so powerfully hated today by heads of state who find out. Such hatred does not serve American interests well.

[xxii] Shankar, S. (2016, February 23). WikiLeaks Says US Spied on Meetings of UN Chief, Angela Merkel, Benjamin Netanyahu. In the *International Business Times*.

[xxiii] Borger, J. (2013, September 24) Brazilian President: US Surveillance a 'Breach of International Law' in *The Guardian*, (London, UK).

[xxiv] "Embassy Espionage: The NSA's Secret Spy Hub in Berlin" (2013) by Spiegel staff in *Spiegel Online* (English) can be accessed at: http://www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html . The original was published as Das Nest in *Der Spiegel*, (2013, October 28).

[xxv] BBC World Service (2016, March 5) *The Inquiry*, "How did Governments Lose Control of Encryption?" accessible at: http://www.bbc.co.uk/programmes/p03kd3k1 .

[xxvi] The whole story of German "Enigma" machines and the struggle by British and US intelligence to a) capture one and b) figure out how to use them to decode military communications is one of the great foundational stories of signals intelligence and the birth of computers. It is one of the best spy stories ever, and a tremendous victory of good guys, girls and intelligence operators (many of whom sacrificed their lives) to defeat a truly evil empire. The particular aspect of how they gave birth to modern computers is well told in a movie *The Imitation Game* (2014)

about real-life British cryptanalyst Alan Turing who developed a "Turing Machine" (which was arguably the first computer) at Bletchley Park to break the cyphers created by the Enigma machine.

[xxvii] Cole, D. We Kill People Based on Metadata (2014, May 10) in *The New York Review*. The title is based on an answer General Michael Hayden gave to a question at a debate with Cole at Johns Hopkins University that year. The article can be accessed at: http://www.nybooks.com/daily/2014/05/10/we-kill-people-based-metadata/

[xxviii] The Phoenix program started as a counterintelligence program in Vietnam that degenerated into nightly raids to torture suspected Viet Cong rebels into revealing comrades in their rebellion. Many of those were then killed, after generating new lists of people to capture, interrogate and kill on subsequent nights. The North Vietnamese estimated that 41,000 people died this way, and Bill Colby (then CIA Station Chief in Saigon, later Director of US Central Intelligence) estimated we killed 26,000 Vietnamese during this program in his book *Honorable Men: My Life in the CIA* (1978) New York NY: Simon & Schuster. This sets upper and lower limits for estimating casualties.

[xxix] A good update on current FBI suppression of domestic political dissent is found in "How the FBI Polices Dissent and Why it Matters in the Encryption Debate," by Chip Gibbons in *Truthout*, March 5, 2016, at: http://www.truth-out.org/news/item/35048-how-the-fbi-polices-dissent-and-why-it-matters-in-the-encryption-debate .

[xxx] An excellent and quick review of COINTELPRO is at https://en.wikipedia.org/wiki/COINTELPRO .

[xxxi] Goldman, J. (2006). *Ethics of Spying: A Reader for Intelligence Professionals.* (Lanham, Maryland: Scarecrow Press).

[xxxii] Andregg, M. (2007). *Intelligence Ethics: The Definitive Work of 2007**, (St. Paul, MN: Ground Zero Center for the Study of Intelligence and Wisdom). This edited work included essays from 14 authors and 6 countries.

[xxxiii] Olson, J. (2006). *Fair Play: The Moral Dilemmas of Spying*, (Washington D.C.: Potomac Books).

[xxxiv] Goldman, J. (2012). *International Journal of Intelligence Ethics,* Vol. 3, No. 2, Fall/Winter, 2012. This issue focused on a thesis advanced by Goldman in Andregg's 2007 reader which introduced the term "Ethics Phobia."

[xxxv] The positive view of this World War II intelligence and special operations group that gave rise to the CIA can be found at their alumni society, the OSS Society, at: http://www.osssociety.org/. One point deserves emphasis here. In my experience all such groups start out with truly the best of intentions to protect something of real value including their countries, their families, and even universal values like freedom and justice. But like all people, groups are not perfect. And when secrecy and killing are parts of their portfolio, some disastrous mistakes occur. But alumni organizations almost always lionize the good parts, and forget the bad parts, like many individuals do.

[xxxvi] *Project MKUltra, the Central Intelligence Agency's Program of Research into Behavioral Modification. Joint Hearing before the Select Committee on Intelligence and the Subcommittee on Health and Scientific Research of the Committee on Human Resources, United States Senate, Ninety-Fifth Congress, First Session*, (1977, August 8) US Government Printing Office. My own University of Minnesota hospitals were part of that program, and tortured a 17 year old girl by forced exposure to massive doses of LSD for 4 days until she became catatonic (testimony of psychometrist Mary Ray to the US Congress in 1975, and confirmed by me when I worked there some years later). A PDF is accessible at: http://www.nytimes.com/packages/pdf/national/13inmate_ProjectMKULTRA.pdf

[xxxvii] "KUBARK Counterintelligence Interrogation," was produced by the CIA in July of 1963. This manual includes unambiguous torture techniques, many used again from 2001 – 2008 at least. The National Security Archives of George Washington University, maintains a copy accessible at: http://nsarchive.gwu.edu/NSAEBB/NSAEBB122/CIA%20Kubark%201-60.pdf

[xxxviii] Colby, Wm., and Peter Forbath (1978). *Honorable Men: My Life in the CIA*, New York, NY: Simon and Schuster, provides one view on that. Guenter Lewy provides a more objective view in *America in Vietnam*, (1978) London: Oxford University Press.

[xxxix] "Psychological Operations in Guerrilla Warfare" drew on lessons learned in Vietnam but was produced by the CIA in 1983 for a secret war in Nicaragua. The code named author was "Tayacan." A pdf version is accessible at: http://fas.org/irp/cia/guerilla.htm but I recommend a print version with commentary by Joanne Omang and Aryeh Neier (1985) *Psychological Operations in Guerrilla Warfare: The CIA's Nicaragua Manual*, New York: Vintage Books.

[xl] Strasser, S. (2004). *The Abu Ghraib Investigations: The Official Reports of the independent panel and the Pentagon on the Shocking Prisoner Abuse in Iraq*, New York, NY: Public Affairs LLC.

[xli] Gibney, A. (2007). *Taxi to the Dark Side* won the 2007 US Film Academy Award for Best Documentary for many reasons. The son of a career interrogator for the US military, Gibney knew what had been considered the proper way for honorable men to interrogate prisoners under the US Military Rules of War. He interviewed several of the people directly involved in ultimately beating a completely innocent man to death in Afghanistan, thinking that he

might be an insurgent. That unfortunate man was one of at least 98 US prisoners of war who died in custody there and in Iraq, 34 of whom were classified as homicides or probable homicides by U.S. government investigators.

[xlii] *The Senate Intelligence Committee Report on Torture: Committee Study of the Central Intelligence Agency's Detention and Interrogation Program*, forward by Senator Dianne Feinstein (2014). Melville House published one-tenth of the official report cleared for public release in December, 2014. Approximately 9/10ths remains secret.

[xliii] This paragraph includes some references to Army uses of torture as well as CIA, but it bears mention that the Army's gold-standard rules on proper interrogation methods were thrown out by CIA enthusiasts at Guantanamo Bay, Cuba, and specifically transferred to the Iraq theater of operations by Maj. General Geoffrey D. Miller over strenuous objections from experienced military interrogators who knew why those rules were originally adopted – to protect our POWs from similar abuse by enemies enraged by our use of torture against their fighters.

[xliv] The National Counter Terrorism Center's description of insider threats is: http://www.ncsc.gov/issues/ithreat/ The NCTC encourages companies to look for insider threats at all times, much like government agencies now do.

[xlv] See White House press release at: https://www.whitehouse.gov/the-press-office/2011/10/07/executive-order-13587-structural-reforms-improve-security-classified-net .

[xlvi] Ackerman, S. and Ed Pilkington (2015, March 16). Obama's War on Whistleblowers Leaves Administration Insiders Unscathed, in *The Guardian* (London, UK).

[xlvii] The origins of this much quoted phrase are in Aristotle's "Nicomachean Ethics" specifically page 42, 1107a, lines 1-5 of book 2, chapter vi. His longer phrasing has been condensed by many others to its core meaning.

[xlviii] Hummel, R. P. (2015). *Understanding Bureaucracy*, especially Chapter 3 on the Psychology of Bureaucracies, pp. 123-160, where the author states explicitly that "Bureaucrats are asked to become people without conscience" on item 1 of page 124. He draws heavily on the pioneer of sociology, Max Weber, and on many cited studies since WW II. Accessible at: http://www.utexas.edu/research/cswr/survey/surveyresources/Admin/Hummel3.pdf

[xlix] Cole, D. (2009, Oct. 8). The Torture Memos: the case against the lawyers, in *The New York Review of Books*.

[l] Weiner, T. (2008). *Legacy of Ashes,* New York, NY: Anchor Publishing.